International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 9 Issue 5, Sep-Oct 2025 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Risk-Based Approach to Computerized System Validation

Kirankumar Patel

Bachelor of Pharmacy (BPharm) and Master's in Information Technologies Management (MSITM)

ABSTRACT

The purpose of this review is to provide comprehensive guide for Computer System Validation (CSV) for the life sciences industry. Computerized System Validation (CSV) is a fundamental practice in the regulated life science industry, serving as the backbone for maintaining product quality, patient safety, and data integrity in an era of global digitalization. The traditional, resource-intensive "box-tickling" approach to CSV struggles to keep pace with the increasing complexity of modern computer systems, evolving regulatory landscapes, and the constraints of time and budget. This review explores the transition to a more strategic, risk-based approach to CSV, which prioritizes validation activities based on their potential impact on GxP-regulated processes. The internationally recognized GAMP 5 framework is presented as a cornerstone of this methodology, providing a systematic approach to categorize software and tailor validation activities accordingly. Also, this review article outlines the purpose of CSV, the challenges it faces, and the specific types of GxP-regulated systems subject to validation. It further details the phases of a risk-based CSV lifecycle, from initial GxP impact and supplier assessments to change control, emphasizing the shift from extensive, redundant testing towards a more focused, critical thinking-based effort. Ultimately, adopting a risk-based approach enhances efficiency, reduces the burden of documentation, and reinforces data integrity and regulatory compliance.

How to cite this paper: Kirankumar Patel "Risk-Based Approach to Computerized System Validation" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-9 | Issue-5, October 2025, pp.223-232, URL: www.ijtsrd.com/papers/ijtsrd97461.pdf

IJTSRD97461

Copyright © 2025 by author (s) and International Journal of Trend in Scientific Research and Development Journal. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0) (http://creativecommons.org/licenses/by/4.0)

KEYWORDS: *Computerized System Validation, Risk based Approach, Qualification, GAMP, Validation.*

I. Definition

A. Validation: Validation means "confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use can be consistently fulfilled"

B. Computer System: A system containing one or more computers and associated software.

C. Computerized System: The computerized system consists of hardware, software, and network components, together with controlled functions and associated documentation.

D. Computer System Validation: Per FDA software validation guidance "confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses, and that the requirements implemented through software can be consistently fulfilled.

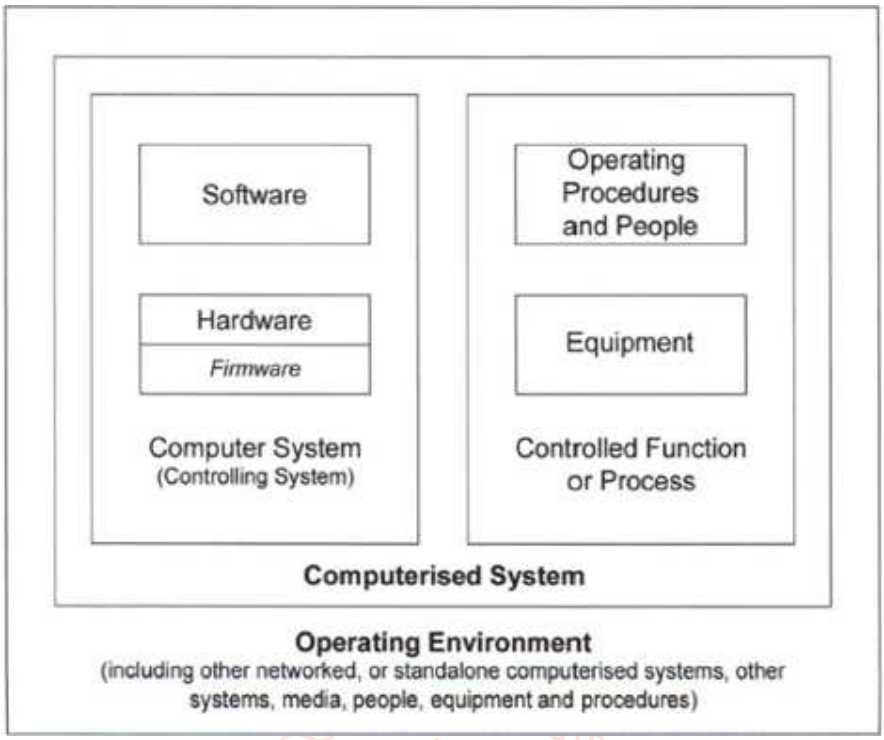

Figure 1

II. Introduction

In Pharma 4.0, Computerized System Validation (CSV) is back bone of the life science industry. CSV is critical in regulated industries that ensure systems operate consistently and produce results that meet predetermined specifications. It is a regulatory necessity for industries like pharmaceutical manufacturing, medical devices, and clinical trials, bridging the gap between technology and regulatory compliance. In industry, where products can directly impact patient health, CSV is crucial [1-2].

III. Purpose of CSV

A. To meet Product Quality and Patient's Safety: CSV ensures computerized system used in the drug development, manufacturing, testing, Packaging and distribution functions correctly and consistent in production of safe and effective products.

B. Regulatory Compliance: Regulated industries must adhere to stringent standards, such as those set by the FDA (e.g., 21 CFR Part 11) or the European Medicines Agency (e.g., EU Annex 11.CSV ensures that computer systems meet these requirements, minimizing the risk of non-compliance, fines, and other penalties.

C. Data Integrity and Security: Computer systems play a vital role in handling sensitive data of the product manufacturing. CSV verifies that data remains accurate, consistent, and secure throughout its product lifecycle by preventing unauthorized access, alterations, or loss.

D. Operational Efficiency: Validated computerized systems are more reliable and function effectively, leading to smoother workflows, reduced downtime, and increased efficiency in overall operations.

E. Audit Readiness and Traceability: CSV involves thorough documentation of the validation process, including plans, specification, protocols, test results, and reports. This comprehensive documentation provides readily available as evidence for regulatory inspections and audits, making the process smoother and ensuring traceability of all system-related activities.

F. Trust and Confidence: CSV demonstrates that computer systems have undergone rigorous validation which gained trust from regulators, partners, and patients, strengthening a company's reputation for quality and reliability [3-5].

IV. Challenges to CSV

A. Complexity of Systems: Modern computer systems often involve intricate networks of software, databases, and cloud services, making it difficult to validate the entire system's integrity.

B. Time and Resource Constraints: CSV can be expensive and time-consuming, requiring significant investments in personnel training.

C. Evolving Regulations: Regulatory bodies like the FDA and EMA continually update guidelines, requiring companies to stay informed and adapt their validation processes.

D. Documentation Requirements: Rigorous documentation is crucial for demonstrating compliance, but can be a burden, especially for complex systems.

E. Cybersecurity Risks: New computer systems introduce new cybersecurity risks which require careful assessment and mitigation strategies.

F. Lack of Expertise: CSV requires specialized knowledge and skills, which may not be readily available within all organizations.

G. Outdated Approaches: A prescriptive Largely box- tickling approach where all computer systems are treated same regardless of the level of risk [6-7].

V. Which systems are subject to CSV

The computerized systems which are used in regulated activities such as Good Clinical Practice (GCP), Good Manufacturing Practice (GMP), Good Laboratory Practice (GLP), Good Distribution Practice (GDP) be subject to CSV are listed below for instance:

- **Pharmaceutical or Biotechnology:**
  - Manufacturing Execution Systems (MES)
  - Laboratory Information Management Systems (LIMS)
  - Enterprise Resource Planning (ERP) systems
  - Quality Management Systems (QMS)
  - Clinical Trial Management Systems (CTMS)
  - Batch Record Systems
  - Chromatography Data System (CDS)
  - Building Management Software (BMS)
- **Healthcare:**
  - Clinical Trial Monitoring Systems
  - Electronic Health Records (EHR)
- **Meical Device:**
  - Software used in device manufacturing and operation
  - Software used as component, Part or accessory of a medical device or itself.
    E.g. Radiation Treatment Control Software, Infusion Pump, Software, Pacemaker Software, Blood Donor Management Software [7-9].

VI. Consequences of CSV failure

- **Warning Letter:** Regulatory bodies like the U.S. Food and Drug Administration (FDA) and the European Medicines Agency (EMA) can issue warning letters for non-compliance with validation standards.
- **Consent decree or Injunction:** Legal action results in a consent decree, a court-ordered agreement to bring processes into compliance, or an injunction, a court order preventing a company from distributing a product.
- **Product seizure:** Due to CSV Non-compliance, Regulatory agencies can shut down production facilities or order the seizure of products that are suspected of being "adulterated" or "misbranded" due to faulty computer systems.
- **Import restrictions:** Overseas drug manufacturer does not allow to sell product in
- **Clinical hold:** Delay in approval of new products or facilities: For new products, failure to validate critical systems can lead to a delay in, or rejection of, a product application until the systems are brought into compliance.
- **Rejection of application**: A Computer System Validation failure can jeopardize the regulatory approval process for new drugs or devices.
- **Debarment:** Debarment is a serious legal action that prohibits individuals and entities from participating in certain activities within the FDA-regulated industry.
- **Criminal prosecution:** In cases of severe, knowing, or willful violations, CSV failure can escalate to criminal prosecution.
- **Operational inefficiencies:** Companies with inadequate CSV practices experience higher rates of system-related deviations and process failures, leading to inefficient operations [9-13].

VII. Risk based CSV approach

A risk-based approach to Computer System Validation (CSV) focuses validation efforts on areas that pose the greatest risk to product quality, patient safety, and data integrity. Risk based validation helps to reduce the burden of documentation while performing the CSV. and align with regulatory guidance such as FDA's Computer Software Assurance (CSA) and GAMP 5. ISPE GAMP 5 provides a globally respected, risk-based framework for validating computerized systems in GxP-regulated industries. GAMP 5 supports the key principles including critical thinking, risk-based validation and leveraging the supplier testing during CSV.

GAMP has 5 categories for Software:

- **Category 1 –** Infrastructure software (e.g. operating systems, Database Managers)
- **Category 3 –** COTS -non-configurable software (e.g. Lab instruments, and Programmable Logic Controllers (PLCs).
- **Category 4 –** COTS- Configurable software (e.g. Laboratory Information Management Systems (LIMS), Supervisory Control and Data

Acquisition (SCADA) systems, and Enterprise Resource Planning (ERP) systems.)

- **Category 5 –** Bespoke (custom code) software (e.g. custom-built software for controlling production machines or unique electronic batch record systems)

Hardware Categories

- **Category 1 – Standard Hardware Components:** This category refers to hardware that is not custom-built but rather a standard, commercially available component. (e.g. PLC or Controller).
- **Category 2– Custom-built Hardware Components:** This category includes hardware that has been specifically designed and built for a particular purpose. E.g. Printed Circuit Board (PCB)[13-15].

VIII. Why Software categories are important to evaluate the risk?

In Pharma 4.0 emphasize heavily to use digital technology which includes software and hardware. To ensure software operates correctly, it needs to be validated. The validation Efforts are determined by the complexity of the software where GAMP categories play a crucial role in identifying the risk and complexity associated with the software [16].

IX. Computerized System Lifecycle

The Computerized System Lifecycle consists of four major phases as listed below. Below are possible validation activities and deliverables carried out in each phase of computerized system Lifecycle.

The basic framework for the CSV is described below, which is scalable and adjusted based on the complexity of the system.

1. Concept

The following GAMP 5 software and hardware categories are used to establish the validation approach and determine the deliverables:

1.1. GxP Impact Assessment

The GxP impact assessment is carried out to determine if the computerized system has an impact on product quality, patient safety or data integrity. All GxP impact computer systems must comply with applicable regulatory requirements [17-19].

2. Project

2.1. Supplier Assessment

The computerized system supplier must be assessed to determine their suitability to provide a quality system that meets all requirements. Software Supplier will be assessed through their Quality Management System (QMS) and Software Development Life Cycle (SDLC). The assessment may take the form of a basic checklist questionnaire, or an onsite audit, depending on the outcome of the risk assessment [20-22].

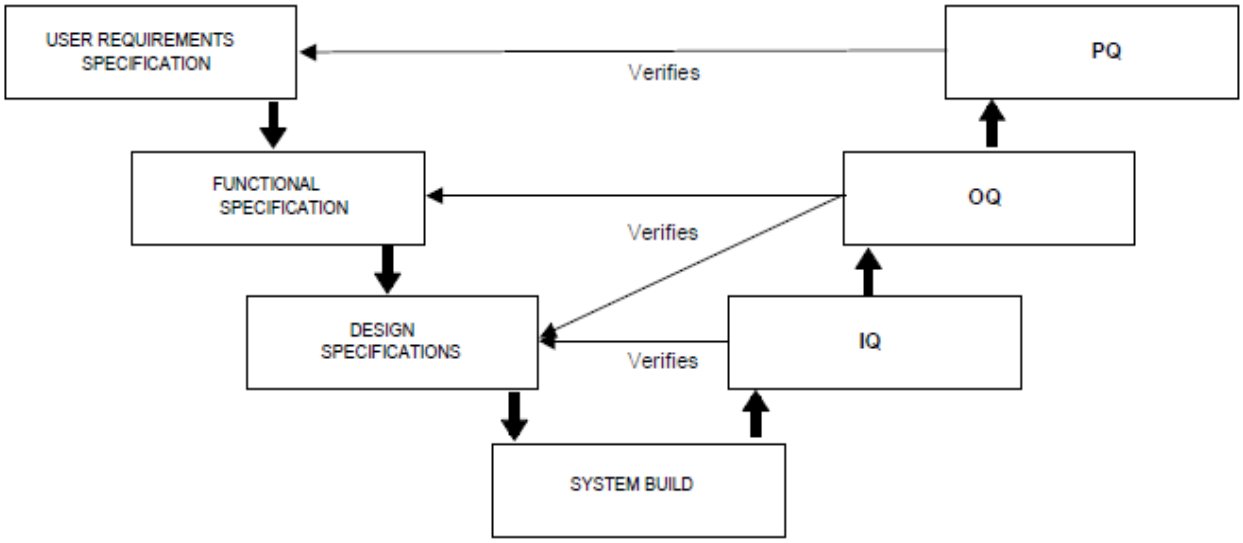

Figure 2

2.2. Service Level Agreement (SLA)

A Service Level Agreement (SLA) documents is an agreement between supplier and regulated company. SLA clearly defines service, document and data ownership and ensures accountability, roles and responsibilities are established. The escalation process should be fully described along with the service performance criteria.

2.3. Change Control

The change Control is a formal process used to manage and control changes to products, processes, facilities, equipment, and documentation. It ensures that all changes are properly assessed for impact, documented, and implemented to maintain product quality, patient safety, and data Integrity.

2.4. Validation Plan (VP)

The Validation Plan (VP) defines the scope, validation approach, system description and boundaries, detail the acceptance criteria and list the deliverables and responsibilities [23-25].

2.5. 21 CFR part 11 Assessment

The 21 CFR part 11 assessment is a process to determine if a computerized system used to manage electronic records and electronic signatures is subject to the requirements of 21 CFR Part 11, the U.S. Food and Drug Administration (FDA) regulation that ensures these electronic records are trustworthy, reliable, and equivalent to paper records and handwritten signatures. The assessment clarifies specific requirements apply to the system, ensuring compliance by implementing controls, audits, and documented procedures for system validation, data integrity, security, and audit trails.

2.6. User Requirements Specification (URS)

The User Requirements Specification (URS) clearly and precisely states what the user wants the system to do. URS also document Intended use of the system and system description. All requirements should be verifiable and unambiguous and uniquely identified such as URS-01. The following areas should be considered [25-27]:

- Operational requirements
- Electronic Record Requirements
- Electronic Signature Requirements
- Interfaces Requirements
- System access and security Requirements
- Data Lifecycle requirements
- Data Integrity Requirements

2.7. Functional Requirements Specification (FS):

The FRS defines the system functionality including how the user and business requirements are satisfied by the computerized system. It is the basis for system design, customization, development and testing. Supplier documentation should be leveraged wherever possible or referenced to FS. FS must be clear how the requirements are met by the URS. The FS may be combined with the URS as a Functional Requirement Specification (FRS) [27-28].

2.8. Risk Assessment (RA)

Risk assessments should be performed at various key stages of the validation process by a multidisciplinary team so that a full understanding of all processes and requirements is covered and considered. This helps to identify and manage risks to patient safety, product quality and data integrity.

A functional risk assessment is performed following approval of the functional specification and/or technical documentation, to identify potential risks. Mitigation activities are then planned to manage the identified risks and allow focusing on critical areas, e.g., by modifying functionality, detailed testing, procedural controls or training.

The risk assessment for computerized systems uses the principles of severity, complexity, and likelihood of occurrence to determine the level of validation.

There are three pillars of risk assessment:

1. **Severity of harm**: This factor evaluates the potential impact of a system failure or data integrity breach on a GxP-regulated process. The analysis considers the consequences for patient safety, product quality, and regulatory compliance.
   - **High severity:** A failure could lead to life-threatening risks to a patient, a product recall, or the submission of erroneous data to a regulatory body.
   - **Medium severity**: The failure could have a significant but non-critical impact, such as a process deviation that needs corrective action.
   - **Low severity:** The impact is minimal, with no direct effect on product quality, patient safety, or data integrity.
2. **Complexity**: Complexity is a measure of how likely a system is to fail or have defects, and it dictates the rigor of the validation activities. A system's complexity is determined by its architecture, configuration, and customization.
   - **High complexity:** Systems with custom code, complex integrations between components, or extensive configuration pose a higher risk of defects and require more rigorous validation.
   - **Medium complexity**: Systems with moderate configurations or integrations carry a medium risk.
   - **Low complexity:** Standard, off-the-shelf software with little to no configuration is considered low risk.
3. **Likelihood of occurrence**: This is the probability that a specific failure will occur. It is influenced by the system's design, complexity, and the effectiveness of controls.
   - **High likelihood:** A failure is very likely due to factors like high-risk functionality, a new or unproven system, or weak controls.
   - **Medium likelihood:** A failure is possible, but not a certainty.
   - **Low likelihood:** A failure is unlikely due to robust design, testing, or effective mitigating controls [29].

2.9. Configuration Specification (CS):

The Configuration Specification details the configuration of the system such as security settings

and how these settings address the requirements in the URS. This may be a standalone document or detailed in the FS. Configuration will be verified as part of the IQ.

2.10. Design Specification (DS):

This activity involves documenting both the hardware and software as a combined document (DS). For some complex system Hardware Design Specification (HDS) and Software Design Specification (SDS) can be separate documents. For less complex system, it can be combined with the FS.

2.11. Design Review:

Design Reviews (DR) are conducted to verify that the DS. The FS meets the requirements defined in the URS and that the requirements can be traced through the design documents in preparation for testing.

2.12. Code Review:

A code review is performed to detect and fix coding errors before the system goes into formal testing. It verifies that the software has been developed following the design and programming standards have been followed.

2.13. Data Migration Plan (DMP)

A Data Migration Plan is created when a system requires data loading from an existing system or the existing system is going to be retired. Data can be manually or automatically loaded/migrated, however, if any critical data has been manually entered, an evaluation should be carried out to ensure its correctness.

2.14. Data Migration Summary Report:

After completion of data migration, Summary report will be generated to summarize the attributes and exceptions observed [30].

2.15. Testing:

Testing is carried out to verify that the system functionality is challenged and tested. The testing or validation approach is described in a test plan as either a section within the validation plan or as a standalone document. Where possible at each stage, any previous testing should be leveraged from supplier, which is defined in the plan.

The installation qualification (IQ), Operational Qualification (OQ), Performance Qualification (PQ) documents are generated against pre-approved specifications. Test cases are written in test steps as instructions to be followed to test whether the system satisfies the defined acceptance criteria appropriate for the test level. A printed copy of the approved test case document is executed, and the test steps are annotated to record the test results. Verification against the expected result defines whether the test step is a pass or fail. Evidence produced during test execution (e.g., reports or screen prints) is attached to allow independent review and approval of the results. Test results are reviewed, summarized, and approved as a standalone test report or as part of the executed protocol [31].

2.15.1. Installation Qualification (IQ)

The Installation Qualification Protocol verifies the proper installation and configuration of a System. This can include ensuring that necessary files have been loaded, equipment has been installed, the necessary procedures have been approved, or the appropriate personnel have been trained. The requirements to properly install the system were defined in the Design Specification. Installation Qualification must be performed before OQ. Depending on your needs and the complexity of the system, Installation Qualification can be combined with Operational Qualification or Performance Qualification.

2.15.2. Operational Qualification (OQ)

The Operational Qualification Protocol is a collection of test cases used to verify the proper functioning of a system. The operational qualification test requirements are defined in the Functional Requirements Specification. Operational Qualification is usually performed before PQ.

2.15.3. Performance Qualifications (PQ)

Performance Qualifications are a collection of test cases used to verify that a system performs as expected under simulated real-world conditions. The performance qualification requirements are defined in the User Requirements Specification. The PQ is performed by end users as the system is being released.

Discrepancies or Exception: When the actual results of a test step in a Test Protocol do not match the expected results, this is called a Deviation or exception. Deviation should include

- **Description** – How the actual results differ from the expected results.
- **Root Cause –** What caused the deviation.
- **Corrective Action –** What changes were made to the testing protocol or the system to correct the deviation.
- **Close Out-** To close the deviation by re-executing the steps or applicable corrective actions.

2.16. Standard Operating Procedures (SOP)/Work instruction:

System Operating Procedures should be written to provide clear unambiguous instructions for end users. User manuals should be leveraged wherever possible.

In some cases, suppliers provided user manuals and technical instruction documents leveraged as needed.

2.17. Training:

End users must be trained to operate the system as needed for GXP use according to SOP or Work Instruction [32].

2.18. Requirements Traceability Matrix:

Traceability Matrix can trace the results of the risk assessment, via the requirements specification, design and through all testing Protocols (IQ, OQ, PQ) to individual test cases.

2.19. Validation Summary Report (VR):

The Validation Report (VR) summarizes the activities carried out during the validation (IQ, OQ, PQ) of computerized System, describes any deviations, with justification, from the Validation Plan (VP), lists any limitations or restrictions on use, summarizes any incidents and details any outstanding and corrective actions. An Interim Validation Report may be issued if all post-go-live activities are not complete.

2.20. Hand Over:

The final transition where the validated system is formally transferred to the operational team, ensuring they have the necessary training, documented procedures, and support structures to maintain the system's compliance and intended use.

3. Operation

The computer system is now in GxP operation phase. For system to maintain the validated status, system's production environment must be kept in a state of control. The following activities will assist in this phase.

3.1. Incident/Deviation Management

The incident/deviation management process defines the requirements for managing incidents/deviations for the entire system lifecycle. It details the recording, analyzing, resolution and closure of faults, anomalies and problems that have been identified during operation of the system. Incident logs should be created for tracking incidents [33].

3.2. Document Management

The document management process defines the lifecycle controls for GxP system documentation including the draft, review, approval, storage, archiving and distribution of documents. It describes how documents are classified, named, numbered, and maintained, and the mechanism for updating them. It applies to both hard copy (paper) and soft copy (electronic) documents.

3.3. Change Management

The Change management process defines how change will be assessed, its impact and control implementation before system release for GxP use. After initial qualification, change will be identified from the release notes and advance notification from software suppliers to identify how changes will affect the existing workflow [34].

3.4. Access and Security Management

The access and security management process defines the requirements for the security and integrity of a system thought end of life. Physical and logical security protection mechanisms should secure the system and data against deliberate or accidental loss, damage or unauthorized change. Access requests and permissions should be defined in Configuration Specifications or system administrator procedure.

3.5. Backup and Restore

Backup and restore is a routine process consisting of copying software, data and electronic records to a separate safe and secure area.

This information is protected, available and when required, able to be restored, uncorrupted in its original format.

3.6. Business Continuity Plan (BCP)

Business Continuity ensures that the crucial functions of a computerized system, especially in regulated industries, can continue to operate during or after a disruptive event like a system failure, cyberattack, or natural disaster. A CSV Business Continuity Plan (BCP) involves assessing risks, creating recovery strategies for the system and its data, establishing clear communication to impacted users, identifying critical system dependencies, and outlining procedures for maintenance, testing, and updating the plan to maintain operational resilience and regulatory compliance [35-36].

3.7. Disaster Recovery Plan (DRP)

DRP into the Computer System Validation (CSV) process to ensure systems can be restored and continue to meet regulatory and business requirements after an incident. This involves developing a comprehensive DRP and establishing recovery objectives like RTOs and RPOs.

3.8. Periodic Review

Periodic reviews are performed to ensure that the computerized system remains validated for its intended use. The review evaluates the compliance status of the entire system and plans any required corrective action activities. The frequency of review depends on such things as system criticality, risk, business impact and complexity [37-38].

3.9. Data Archive and Retrieval

Data archiving is the process of removing data that is no longer actively used to a separate, secure data

storage area for long-term retention. Data that must be retained for regulatory compliance has to be archived and be available for retrieval when required. Records retention requirements should also be considered for the protection and confidentiality of electronic records, including their associated audit trail information.

4. Retirement

4.1. Decommissioning Plan:

A decommissioning plan must be prepared for systems that are to be retired from operational service so that the process is documented and controlled. Assessment is required with regards to the archiving of data and records retention requirements, along with any hardware disposal [39].

Table 1: GAMP Categories and Deliverables

CSV Lifecycle Phase/Deliverables	GAMP Category			
	Category 1	Category 3	Category 4	Category 5
1. Concept				
GXP Impact Assessment	X	X	X	X
2. Project				
Supplier Assessment / SLA	X	X	X	N/A
Change Control (CC)	X	X	X	X
Validation Plan (VP)	X	X	X	X
21 CFR part 11 Assessment	N/A	X	X	X
User Requirements Specification (URS)	X	X	X	X
Functional Requirements Specification (FRS)	N/A	AA	X	X
Risk Assessment (RA)	N/A	N/A	X	X
Configuration Specification (CS)	N/A	N/A	X	X
Design Specification (DS)	N/A	N/A	N/A	X
Design Review	N/A	N/A	N/A	X
Code Review	N/A	N/A	N/A	X
Data Migration	AA	AA	AA	AA
Data Migration Summary Report	AA	AA	AA	AA
Installation Qualification (IQ)	X	X	X	X
Operational Qualification (OQ)	X	X	X	X
Performance Qualification (PQ)	N/A	X	X	X
Requirements Traceability Matrix (RTM)	X	X	X	X
Qualification Report	X	X	X	X
Validation Summary Report (VSR)	X	X	X	X
3. Operation				
Standard Operating Procedure (SOP) or Work Instruction (WI)	N/A	X	X	X
User Manual or Technical Instruction	X	X	X	X
Change Control	X	X	X	X
4. Retirement				
Decommissioning Plan	X	X	X	X

N/A: Not Applicable **AA:** As Applicable **X:** Needed

X. Conclusion

The risk-based CSV approach, guided by frameworks like ISPE's GAMP 5, provides the pathway for this transition by focusing validation efforts on the areas of greatest risk to product quality, patient safety, and data integrity. The adoption of this risk-based methodology offers significant advantages by optimizing resource allocation and reducing unnecessary validation activities for low-risk systems, thereby enhancing efficiency and minimizing costs. It also aligns with modern regulatory guidance, including the FDA's Computer Software Assurance (CSA), which emphasizes critical thinking over prescriptive documentation. By continuously assessing and managing risks throughout the system's lifecycle, this approach builds confidence in the system's reliability and ensures data integrity, which is crucial for regulatory compliance and audit readiness. Ultimately, the move towards a risk-based CSV model is more than just satisfying regulatory requirements; it is about building a more agile, cost-effective, and robust validation process that can

support innovation and growth. By leveraging supplier documentation, tailoring validation activities to risk levels, and embracing critical thinking, the life sciences industry can successfully navigate the complexities of digitalization. This forward-thinking approach ensures that computerized systems remain a dependable cornerstone for producing safe, high-quality products in the digital age, fostering continued trust from regulators, partners, and patients alike.

XI. References

[1] Singh, A., Singour, P., & Singh, P. (2018). Computer system validation in the perspective of the pharmaceutical industry. *Journal of Drug Delivery Therapeutics*, *8*.

[2] de Claire, T., Coady, P., & Stevens, N. Considerations for Computerized System Validation in the 21st Century Life Sciences Sector.

[3] Andrews, J. (Ed.). (2005). *Validating pharmaceutical systems: good computer practice in life science manufacturing*.

[4] Raja, J. R., Kella, A., & Narayanasamy, D. (2024). The essential guide to computer system validation in the pharmaceutical industry. *Cureus*, *16*(8).

[5] Hoffmann, A., Kähny-Simonius, J., Plattner, M., Schmidli-Vckovski, V., & Kronseder, C. (1998). Computer system validation: An overview of official requirements and standards. *Pharmaceutica Acta Helvetiae*, *72*(6), 317-325.

[6] Lopez, O. (2013). Computer Systems Validation. *Encyclopedia of Pharmaceutical Science and Technology, Six Volume Set (Print)*, 615-619.

[7] Oberkampf, W. L., & Roy, C. J. (2010). *Verification and validation in scientific computing*. Cambridge university press.

[8] Yogesh, P., Kamlesh, M., Mohini, B., Phad, R., Ismail, S., & Shivam, L. (2015). Computer system validation: a review. *World Journal of Pharmaceutical Research*, *4*(9), 444-454.

[9] Wingate, G. (Ed.). (2016). Pharmaceutical computer systems validation: quality assurance, risk management and regulatory compliance.

[10] Dhatchanamoorthi, N., & Kamaraj, R. (2020). An Overview on challenges and importance of computer system validation in Pharmaceutical Industry. *Research Journal of Pharmacy and Technology*, *13*(11), 5591-5594.

[11] Bendale, A., Patel, N., Damahe, D. P., Narkhede, S. B., Jadhav, A. G., & Vidyasagar, G. (2011). Computer software validation in pharmaceuticals. *Asian Journal of Pharmaceutical Sciences and Clinical Research*, *1*(2), 27-39.

[12] Rusjan, B. (2020). Computer system validation: Example of quality management system design and process implementation. *Management: Journal of Contemporary Management Issues*, *25*(2), 1-23.

[13] López, O. (2018). *Pharmaceutical and Medical Devices Manufacturing Computer Systems Validation*. Productivity Press.

[14] Sharvani, C., Jain, V., Kumar, H., & HV, G. (2021). Implementation of Good Computer System Validation Practices In Pharmaceutical Industry-A Review.

[15] McDowall, R. D. (1995). Practical computer validation for pharmaceutical laboratories. *Journal of pharmaceutical and biomedical analysis*, *14*(1-2), 13-22.

[16] Maropoulos, P. G., & Ceglarek, D. (2010). Design verification and validation in product lifecycle. *CIRP annals*, *59*(2), 740-759.

[17] Huber, L. (2005). Risk-based validation of commercial off-the-shelf computer systems.

[18] Oberkampf, W. L., Trucano, T. G., & Hirsch, C. (2004). Verification, validation, and predictive capability in computational engineering and physics. *Appl. Mech. Rev.*, *57*(5), 345-384.

[19] Cahilly, M. J. (2005). Validation of Computerized Systems. *BIOTECHNOLOGY AND BIOPROCESSING SERIES*, *29*, 395.

[20] Agalloco, J., & Carleton, F. J. (2008). *Validation of pharmaceutical process* (3rd ed.). Informa Healthcare.

[21] Chitlange, S. S., Chaudhari, P. D., Shirsath, A. E., & Sangshetti, J. N. (*n.d.*). *Pharmaceutical validation* (1st ed.). Suyog Publication and Distributors Pvt. Ltd. (This entry is missing a publication date and page range).

[22] Coombes, P. (2002). *Laboratory systems validation testing and practice*. DHI Publishing, LTD.

[23] Kaner, C., Falk, J., & Nguyen, H. Q. (1999). *Testing computer software*. John Wiley & Sons.

[24] Nash, R. A., & Wachter, A. H. (Eds.). (2003). *Pharmaceutical process validation* (3rd ed.). Marcel Decker.

[25] Potdar, M. A. (*n.d.*). *CGMP for pharmaceuticals, pharmaceutical validation* (3rd ed.). Nirali Prakashan. (This entry is missing a publication date).

[26] Bedson, P., & Sargent, M. (1996). The development and application of guidance on equipment qualification of analytical instruments. In *Accreditation and Quality Assurance*, *1*(6), 265–274. (This is formatted as an article but may have been a book chapter).

[27] Sangeetha, N. K. D., & Balakrishna, P. (2011). Development and validation of a UPLC method for the determination of duloxetine hydrochloride residues on pharmaceutical manufacturing equipment surfaces. *Pharmaceutical Methods*, *2*(3), 161–166.

[28] Strause, S. (2009). Computer system validation—Definition and requirements. *Journal of Validation Technology* (Spring issue), 1–5. (This entry lacks specific volume/issue and may be incomplete).

[29] *GAMP guide, a risk-based approach to complaint GxP computerized systems* (Version 5.0). (July 2022). GAMP Forum.

[30] *GAMP good practice guide,A Risk- Based Approach to testing of GxP systems*. (December 2012). 2nd Edition

[31] Huber, L. (2009). *Analytical instrument qualification and system validation* (Publication No. 5990-3288EN). Agilent Technologies.

[32] Food and Drug Administration. (2001, August). *Guidance for the industry: 21 CFR Part 11; Electronic records; Electronic signatures: Glossary of terms* (Draft). U.S. Department of Health and Human Services.

[33] Food and Drug Administration. (2002, January). *General principles of software validation; Final guidance for industry and FDA staff*. U.S. Department of Health and Human Services.

[34] Food and Drug Administration. (2006, September). *Guidance for industry: Quality systems approach pharmaceutical current good manufacturing regulations*. U.S. Department of Health and Human Services.

[35] Food and Drug Administration. (1996). 21 CFR, Part 211: Current good manufacturing practice for finished pharmaceuticals, sections 21 I. 22: Proposed rules. *Federal Register, 61*, 20104–20115.

[36] *PDA website*. http://www.pda.org

[37] *FDA website: https://www.fda.gov*

[38] *PIC/s* website: https://picscheme.org/en/picscheme

[39] ISPE website: https://ispe.org